In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

In the Claims:
   1. (Currently Amended) A block cipher device for a cryptographically secured digital communication system comprising:
   a pair of first stages connected in parallel and receiving an input data block and a control data block, each first stage defining a respective first data path and comprising
     a sum modulo-two unit responsive to the control data block and the input data block, and
     a first nibble swap unit downstream from said sum modulo-two unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said sum modulo-two unit;
   a diffuser connected in both of the first data paths for mixing data therebetween;
   a key scheduler receiving a key data block and generating a random key data block based thereon;
   a pair of second stages connected in parallel downstream from said first stages and receiving the random key data block, the control data block and output signals from said first stages, each second stage defining a respective second data path and comprising
     a first linear modulo unit responsive to the random key data block, one of the output signals from said first stages, and the control data block for performing a modulo summing operation based on a first modulus q,

3

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

an nth power modulo unit responsive to an
output signal from said first linear modulo unit for
performing an nth power modulo operation based on a
second modulus p, and

a second linear modulo unit responsive to the
random key data block and an output signal from said
n^{th} power modulo unit for performing a modulo summing
operation based on a third modulus r,

each first, second and third modulus q, p and
r being unique from each ~~other,~~ other, and

said pairs of first and second stages each
being selectively configurable so that only one first
data path and only one second data path are operational
while bypassing said diffuser; and

an output stage connected to said second stages for
generating an output data block for the block cipher.

Claim 2 (Cancelled).

3.   (Original) A block cipher device according to
Claim 1 wherein said diffuser is connected in both of the first
data paths between the respective sum modulo-two units and first
nibble swap units.

4.   (Original) A block cipher device according to
Claim 1 wherein each first stage further comprises a
substitution/expansion unit downstream from said first nibble
swap unit and being responsive to an output signal therefrom for

4

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

providing customizable cipher variations.

5.   (Original) A block cipher device according to
Claim 4 wherein each first stage further comprises a second
nibble swap unit downstream from said substitution/expansion unit
and being responsive to an output signal therefrom and the
control data block for reordering the output signal from said
substitution/expansion unit.

6.   (Original) A block cipher device according to
Claim 1 further comprising a nibble interleave unit connected in
both of the first data paths for reordering data therebetween.

7.   (Original) A block cipher device according to
Claim 1 further comprising a substitution unit connected in both
of the first data paths for substituting data therebetween.

8.   (Original) A block cipher device according to
Claim 1 wherein each nth power modulo unit provides an output
signal of predetermined size, with $n>1$ and with $p=2^{K}-X$, where X
is selected such that a greatest common denominator between n and
$(2^{K}-X-1)$ is 1 and K is the predetermined size.

9.   (Original) A block cipher device according to
Claim 1 wherein said key scheduler comprises a pair of look-up
tables for generating the random key data block.

10.   (Original) A block cipher device according to

5

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

Claim 9 wherein said key scheduler further comprises a pair of
shift registers responsive to the received key data block; and
wherein each look-up table is responsive to a corresponding shift
register.

11.   (Original) A block cipher device according to
Claim 10 wherein said key scheduler further comprises a pair of
combiners responsive to outputs from said shift registers and to
outputs from said look-up tables, each combiner combining the
output from a corresponding shift register and the output from a
corresponding look-up table using a modulo-two summing operation,
and each combiner providing a combined data output.

12.   (Original) A block cipher device according to
Claim 1 wherein each second stage further comprises a non-
invertible operation unit downstream from said n^{th} power modulo
unit and being responsive to an output signal therefrom, said
non-invertible operation unit discarding a portion of the output
signal from said n^{th} power modulo unit.

13.   (Currently Amended) A communication system
comprising:
        a block cipher device for converting an input data
block into an output data block, said block cipher comprising
                a pair of first stages connected in parallel
        and receiving the input data block and a control data
        block, each first stage defining a respective data path
        and comprising

6

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____ /

a first unit responsive to the
control data block and the input data block,
and

a second unit downstream from said
first unit and being responsive to an output
signal therefrom and the control data block
for reordering the output signal from said
first unit;

a diffuser connected in both of the data
paths for mixing data therebetween;

a key scheduler receiving a key data block
and generating a random key data block based thereon;

a pair of second stages connected in parallel
downstream from said first stages and receiving the
random key data block, the control data block and
output signals from said first stages, each second
stage defining a respective second data path and
comprising

a first modulo unit responsive to
the random key data block, one of the output
signals from said first stages, and the
control data block for performing a modulo
operation based on a first modulus q,

an nth power modulo unit responsive
to an output signal from said first modulo
unit for performing an nth power modulo
operation based on a second modulus p, and

a second modulo unit responsive to

7

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

the random key data block and an output
signal from said n^{th} power modulo unit for
performing a modulo operation based on a
third modulus r,

each first, second and third
modulus q, p and r being unique from each
~~other;~~ other, and

said pairs of first and second
stages each being selectively configurable so
that only one first data path and only one
second data path are operational while
bypassing said diffuser; and

an output stage connected to said second
stages for generating an output data block for said
block cipher device.

14.   (Original) A communication system according to
Claim 13 wherein said first unit comprises a sum modulo-two unit,
said second unit comprises a nibble swap unit, and said first and
second modulo units comprise first and second linear modulo units
for performing summing operations.

15.   (Original) A communication system according to
Claim 13 wherein said block cipher device operates as an
encrypter.

16.   (Original) A communication system according to
Claim 13 wherein said block cipher device operates as a

8

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

decrypter.

17.   (Original) A communication system according to
Claim 13 further comprising circuitry connected to said block
cipher device so that said block cipher device operates in at
least one of a block cipher feedback mode, a minimum error
propagation mode and a self-synchronizing feedback mode.

Claim 18 (Cancelled).

19.   (Original) A communication system according to
Claim 13 wherein said diffuser is connected in both of the first
data paths between the respective first and second units.

20.   (Original) A communication system according to
Claim 13 wherein each first stage further comprises a
substitution/expansion unit downstream from said second unit and
being responsive to an output signal therefrom for providing
customizable cipher variations.

21.   (Original) A communication system according to
Claim 20 wherein each first stage further comprises a second
nibble swap unit downstream from said substitution/ expansion
unit and being responsive to an output signal therefrom and the
control data block for reordering the output signal from said
substitution/expansion unit.

22.   (Original) A communication system according to

9

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

Claim 13 further comprising a nibble interleave unit connected in
both of the first data paths for reordering data therebetween.

        23.   (Original) A communication system according to
Claim 13 further comprising a substitution unit connected in both
of the first data paths for substituting data therebetween.

        24.   (Original) A communication system according to
Claim 13 wherein each nth power modulo unit provides an output
signal of predetermined size, with n>1 and with $p=2^{K}-X$, where X
is selected such that a greatest common denominator between n and
$(2^{K}-X-1)$ is 1 and K is the predetermined size.

        25.   (Original) A communication system according to
Claim 13 wherein said key scheduler comprises a pair of look-up
tables for generating the random key data block.

        26.   (Original) A communication system according to
Claim 25 wherein said key scheduler further comprises a pair of
shift registers responsive to the received key data block; and
wherein each look-up table is responsive to a corresponding shift
register.

        27.   (Original) A communication system according to
Claim 26 wherein said key scheduler comprises a pair of combiners
responsive to outputs from said shift registers and to outputs
from said look-up tables, each combiner combining the output from
a corresponding shift register and the output from a

                                10

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

corresponding look-up table using a modulo-two summing operation,
and each combiner providing a combined data output.

28.   (Original) A communication system according to
Claim 13 wherein each second stage further comprises a non-
invertible operation unit downstream from said n^{th} power modulo
unit and being responsive to an output signal therefrom, said
non-invertible operation unit discarding a portion of the output
signal from said n^{th} power modulo unit.

29.   (Currently Amended) A method for converting an
input data block into an output data block for a
cryptographically secured digital communication system, the
method comprising:
    providing the input data block, a control data block
and a random key data block to parallel data paths in the digital
communication system;
    combining the control data block and the input data
block within each data path to provide a first data output signal
for each data path;
    transposing segments of the first data output signal
within each data path in response to the control data block to
provide a second data output signal within each data path;
    mixing data between the parallel data paths;
    performing a first linear modulo operation based on a
modulus q within each data path in response to the second data
output signal, the random key data block and the control data
block to provide a third data output signal within each data

11

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

path;

performing an nth power modulo operation based on a
second modulus p within each respective data path in response to
the third data output signal to provide a fourth data output
signal within each data path; ~~and~~

performing a second linear modulo operation
based on a third modulus r within each respective data path in
response to the random key data block and the fourth data output
signal to provide an output data block, each first, second and
third modulus q, p and r being unique from each ~~other.~~ other; and

the cryptographically secured digital communication
system being selectively configurable so that only one data path
is operational while mixing of the data is bypassed.

Claim 30 (Cancelled).

31.   (Original) A method according to Claim 29 further
comprising performing a substitution/expansion operation within
each data path on the second data output signal to provide
customizable cipher variations.

32.   (Original) A method according to Claim 31 further
comprising performing a nibble swap operation within each data
path on the customizable cipher variations in response to the
control data block for reordering the customizable cipher
variations.

33.   (Original) A method according to Claim 32 further

12

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

comprising performing a nibble interleave operation for
reordering data between the data paths for the reordered
customizable cipher variations.

34.   (Original) A method according to Claim 33 further
comprising performing a substitution operation after the nibble
interleave operation for substituting the reordered customizable
cipher variations between the parallel data paths.

35.   (Original) A method according to Claim 29 wherein
each nth power modulo operation provides an output signal of
predetermined size, with n>1 and with $p=2^K-X$, where X is selected
such that a greatest common denominator between n and (2^K-X-1) is
1 and K is the predetermined size.

36.   (Original) A method according to Claim 29 wherein
the random key data block is generated by a key scheduler
comprising a pair of look-up tables.

37.   (Original) A method according to Claim 36 wherein
the key scheduler further comprises a respective shift register
associated with each look-up table.

38.   (Original) A method according to Claim 37 wherein
the key scheduler further comprises a pair of combiners
responsive to outputs from the shift registers and to outputs
from the look-up tables, each combiner combining the output from
a corresponding shift register and the output from a

13

In re Patent Application of:
KURDZIEL
Serial No. **110/792,236**
Filed: **March 03, 2004**
_____/

corresponding look-up table using a modulo-two summing operation,
and each combiner providing a combined data output.

14